CLAIMS

In the Claims:

1. A method comprising:

modifying an original header associated with an original data packet wherein key information is added;

encrypting original data associated with the original data packet in response to the key information; and

forming an encrypted data packet including the modified header and the encrypted data,

wherein the encrypted data packet is a same size as the original data packet.

2. The method according to claim 1 further comprising receiving a session identifier.

3. The method according to claim 2 wherein the modifying further comprises modifying the original header in response to the session identifier.

4. The method according to claim 1 wherein the modifying further comprises replacing the fragmentation identification and fragment offset of the original header with a mixing key and an offset.

5. The method according to claim 1 wherein the original data packet and the encrypted data packet utilize Internet Protocol version 4.

6. A system comprising:

means for modifying an original header associated with an original data packet wherein key information is added;

means for encrypting original data associated with the original data packet in response to the key information; and

means for forming an encrypted data packet including the modified header and the encrypted data,

wherein the encrypted data packet is a same size as the original data packet.

7. A method comprising:

distributing a secured session identifer from a KDC to a sender computer and a receiver computer wherein the secured session identifier allows the receiver computer and the sender computer to establish a secure communication session;

storing access rights in the KDC wherein the access rights are associated with the secured sessand identifier; and

obtaining an encryption key via the secure session identifier from the KDC.

8. The method according to claim 7 further comprising obtaining discretionary access rights from the KDC for use with the secured session identifier between the sender computer and the receiver computer.

9. A method comprising:

generating a large number of unique random keys for each encrypted IP packet; and

transmitting the large number of unique random keys to a sender computer and a receiver computer, wherein a transmission overhead from a KDC is reduced.